

# EXPLICIT COUNTING OF IDEALS AND A BRUN-TITCHMARSH INEQUALITY FOR THE CHEBOTAREV DENSITY THEOREM

KORNEEL DEBAENE

**ABSTRACT.** We prove a bound on the number of primes with a given splitting behaviour in a given field extension. This bound generalises the Brun-Titchmarsh bound on the number of primes in an arithmetic progression. The proof is set up as an application of Selberg's Sieve in number fields. The main new ingredient is an explicit counting result estimating the number of integral elements with certain properties up to multiplication by units. As a consequence of this result, we deduce an explicit estimate for the number of ideals of norm up to  $x$ .

## 1. INTRODUCTION AND STATEMENT OF RESULTS

Let  $q$  and  $a$  be coprime integers, and let  $\pi(x, q, a)$  be the number of primes not exceeding  $x$  which are congruent to  $a \pmod q$ . It is well known that for fixed  $q$ ,

$$\lim_{x \rightarrow \infty} \frac{\pi(x, q, a)}{\pi(x)} = \frac{1}{\phi(q)}.$$

A major drawback of this result is the lack of an effective error term, and hence the impossibility to let  $q$  tend to infinity with  $x$ . The Brun-Titchmarsh inequality remedies the situation, if one is willing to accept a less precise relation in return for an effective range of  $q$ . It states that

$$\pi(x, q, a) \leq \frac{2}{\phi(q)} \frac{x}{\log x/q}, \quad \text{for any } x \geq q.$$

While originally proven with  $2 + \varepsilon$  in place of 2, the above formulation was proven by Montgomery and Vaughan [14] in 1973. Further improvement on this constant seems out of reach, indeed, if one could prove that the inequality holds with  $2 - \delta$  in place of 2, for any positive  $\delta$ , one could deduce from this that there are no Siegel zeros. However, improvements concerning the factor  $\frac{1}{\log x/q}$  have been made, we refer to [13] for an overview of the state of the art.

A vast generalisation of the choice of a modulus  $q$  and a residue class  $a$ , is the choice of a Galois extension  $L/\mathbb{Q}$  with Galois group  $G$ , and a conjugacy class  $C \subseteq G$ . Define

$$\pi_C(x, L/\mathbb{Q}) = |\{p \leq x \mid p \text{ unramified in } L/\mathbb{Q}, \text{Frob}_{L/\mathbb{Q}}(p) \in C\}|,$$

the number of primes not exceeding  $x$  with splitting behaviour in  $L/\mathbb{Q}$  determined by  $C$ . The famous Chebotarev Density Theorem gives for fixed  $L$  the asymptotic equivalence

$$\pi_C(x, L/\mathbb{Q}) \sim \frac{|C|}{|G|} \frac{x}{\log x}.$$

An version of this result with effective error terms was first given by Lagarias and Odlyzko [9], in the range  $\log x \geq 10[L : \mathbb{Q}](\log |\Delta_L|)^2$ . Inspired by the Brun-Titchmarsh inequality, one can look for upper bounds which are off only by a constant factor, with a range of validity as wide as possible. In this respect, Lagarias, Montgomery and Odlyzko [8] proved that

$$(1) \quad \pi_C(x, L/\mathbb{Q}) \ll \frac{|C|}{|G|} \frac{x}{\log x},$$

when  $\log x \gg (\log |\Delta_L|)(\log_2 |\Delta_L|)(\log_3 |\Delta_L|)$ . A recent paper by Thorner and Zaman [22] gives a substantial improvement on the range where the inequality holds, using state-of-the-art information on the location of the zeros of Hecke  $L$ -functions. Consider an abelian subgroup  $H \leq G$  such that  $H \cap C$  is not empty, and let  $K$  be the fixed field of  $H$ , of degree  $n$ . For a character  $\chi \in \hat{H}$ , let  $\mathfrak{f}_\chi$  be the conductor, and define

$$\mathcal{Q} = \max_{\chi} \{N_{K/\mathbb{Q}}(\mathfrak{f}_\chi) \mid \chi \in \hat{H}\}.$$

Their result is then that the inequality (1) holds in the range  $x \geq 2|\Delta_K|^{163}\mathcal{Q}^{123} + |\Delta_K|^{55}\mathcal{Q}^{87}n^{68n}$ . They also proved a stronger version, where the unspecified constant factor in (1) is replaced by 2 plus an error term, which is valid in a similar but slightly smaller range.

The main result in this paper is the following explicit bound on  $\pi_C(x, L/\mathbb{Q})$ .

**Theorem 1.** *Let  $L/\mathbb{Q}$  be a Galois extension with Galois group  $G$ , and let  $C \subseteq G$  be a conjugacy class. Let  $H$  be an abelian subgroup of  $G$  such that  $H \cap C \neq \emptyset$ , and let  $K$  be the fixed field of  $H$ , of degree  $n$ . Let  $\mathfrak{f} \subseteq \mathcal{O}_K$  be the conductor of  $L/K$ . Define the constant*

$$c_K = n^{31n^3} (\text{Reg}_K h_K)^3 (1 + \log \text{Reg}_K h_K)^{3(n-1)^2} [L : K]^n N(\mathfrak{f})^n \kappa_K^{-2n}.$$

*Then, for all  $x$  with  $x(\log x)^{-5n^2} \geq c_K$ , we have*

$$\pi_C(x, L/\mathbb{Q}) \leq \frac{|C|}{|G|} \left( 2 + \frac{41n^2 \log \log(x)}{\log(x/c_K)} \right) \frac{x}{\log(x/c_K)}.$$

*Remark.* In terms of the discriminant  $\Delta_K$ , our result gives a wider range than the previous results. By the analytic class number formula,  $\text{Reg}_K h_K$  is interchangeable with  $\sqrt{|\Delta_K|}$  up to a factor bounded in terms of  $n$  and the residue  $\kappa_K = \text{res}_{s=1} \zeta_K(s)$ . Stark [21] gave an effective (but unfortunately not explicit) lower bound for the residue, namely that there is an effective absolute constant  $c$  such that  $\kappa_K \geq \frac{c}{(n!)n|\Delta_K|^{1/n}}$ , where  $n|\Delta_K|^{1/n}$  can be replaced by  $\log |\Delta_K|$  if  $K$  has no quadratic subfield, and  $n!$  can be dropped if  $K$  has a normal tower over  $K$ . So all in all, our result gives a Brun-Titchmarsh bound in the range  $x \gg_{n, [L:K], N(\mathfrak{f}), \varepsilon} |\Delta_K|^{7/2-3/n+\varepsilon}$ . In situations where the discriminant of  $K$  dominates the other factors, this is superior to the hitherto widest known range given by [22].

The proof follows a completely different path than the previous results mentioned on  $\pi_C(x, L/\mathbb{Q})$ . In particular, we stress that we do not use any analytic information on zeta functions or their zeros. The proof is built up in the following stages. First and foremost, we develop an explicit counting method to count the number of integral elements, with certain properties, of norm up to  $x$  and up to multiplication by units. This is achieved in Theorem 11, by translating this counting problem

to a lattice point counting problem and applying a Lipschitz argument. We take particular care to minimize the field constants appearing, by employing the so-called Schmidt's partition trick, and by carefully treating the occurring successive minima. The utility of this explicit counting result will be twofold. Firstly, it allows us to set up an explicit Selberg sieve in number fields, and secondly, through Artin's reciprocity law, the primes with given splitting behaviour can be expressed as integral elements with certain properties, which our counting result can estimate.

To illustrate the strength of our counting result, we mention that one natural and immediate application is the following explicit estimate for the number of ideals of bounded norm.

**Corollary 2.** *Let  $K$  be a number field of degree  $n$ , and let  $a_k$  be the number of ideals of norm  $k$ . Then, for all  $x \geq 1$ ,*

$$\sum_{k \leq x} a_k = \kappa_K x + O^* \left( n^{10n^2} (\text{Reg}_K h_K)^{1/n} (1 + \log \text{Reg}_K h_K)^{\frac{(n-1)^2}{n}} x^{1-\frac{1}{n}} \right)$$

*Remark.* One may again rephrase the constant  $\text{Reg}_K h_K$  in terms of the discriminant  $\Delta_K$ , using the analytic class formula and the bound by Louboutin [12]  $\kappa_K \leq (\frac{e \log |\Delta_K|}{2(n-1)})^{n-1}$ , to bound the error term by  $\ll_{n,\varepsilon} |\Delta_K|^{\frac{1}{2n}+\varepsilon} x^{1-\frac{1}{n}}$ . Thus one can get a meaningful estimate for  $x$  as small as  $\gg_{n,\varepsilon} |\Delta_K|^{1/2+\varepsilon}$ .

The quality of the error term is to be compared with what zeta function methods would yield. We would get roughly the same bounds by an application of Perron's formula with the convexity bound  $\zeta_K(\frac{1}{2} + it) \ll (|\Delta_K|(1 + |t|)^n)^{1/4+\varepsilon}$ . Hence, better bounds could be given in situations where a suitable subconvexity result is known, e.g. when  $K$  is abelian. For general number fields  $K$ , the best result in terms of  $x$  is due to Lao [11], who uses the subconvexity bound  $\zeta_K(\frac{1}{2} + it) \ll_K (1 + |t|)^{n/6+\varepsilon}$  (which follows from Kaufmans work [7]) to produce an estimate with error term  $O_K(x^{1-\frac{3}{n+6}+\varepsilon})$ . However, this result does not specify the dependence on the field constants.

This corollary generalises the result for quadratic fields proven by Schmidt [20], namely that

$$\sum_{k \leq x} a_k = \kappa_K x + O \left( (\text{Reg}_K h_K)^{1/2} (\max(1, \log \text{Reg}_K h_K))^{1/2} x^{1/2} \right),$$

with some absolute implied constant. Widmer [23] proved a comparable result for number fields of fixed degree, working however in a more general setting, counting points of bounded height in projective space over  $K$ . His work would imply an error term  $O_n(\text{Reg}_K h_K x^{1-\frac{1}{n}})$  with constant depending only on the degree. That same error term would be implied in the PhD thesis of Gao [4].

## 2. NOTATION

Let  $K$  be a number field of discriminant  $\Delta_K$  and of degree  $n$ , with  $r_1$  real embeddings and  $r_2$  complex embeddings, so that  $n = r_1 + 2r_2$ . Let  $\sigma_1, \dots, \sigma_{r_1}$  be the real embeddings, and let  $(\sigma_{r_1+1}, \sigma_{r_1+r_2+1}), \dots, (\sigma_{r_1+r_2}, \sigma_{r_1+2r_2})$  be the pairs of complex embeddings. Choose a system of  $r = r_1 + r_2 - 1$  fundamental units in the ring of integers  $\mathcal{O}_K$ , denoted by  $\varepsilon_1, \dots, \varepsilon_r$ . Dependent on this system of

fundamental units, we consider the group of non-torsion units  $U_K = \langle \varepsilon_1, \dots, \varepsilon_r \rangle$ , and we define the positive constants

$$(2) \quad m_j = \lceil \max_i |\sigma_i(\varepsilon_j)| \rceil.$$

Let  $\text{Reg}_K$  be the regulator,  $h_K$  the class number, and  $\kappa_K$  the residue of the Dedekind-zeta function  $\zeta_K(s)$ .

We will reserve the dummy variables  $i$  and  $j$  for specific uses, to make the notation more transparent. The embeddings will always be indexed by  $i$ , whereas the units will be indexed by  $j$ .

Recall the Minkowski embedding

$$\begin{aligned} \phi : K &\rightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \\ \alpha &\mapsto (\sigma_1(\alpha), \dots, \sigma_{r_1+r_2}(\alpha)). \end{aligned}$$

We will identify the image space  $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ , which is called Minkowski space, with  $\mathbb{R}^n$ , by taking real and imaginary parts in the last  $r_2$  coordinates. We will denote by  $\|\cdot\|$  the euclidean norm, where  $|\cdot|$  is the usual absolute value on  $\mathbb{R}$  or  $\mathbb{C}$ . Whenever we write a product of two vectors, componentwise multiplication is what is meant. Define  $e_i = 1$  for  $i = 1, \dots, r_1$  and  $e_i = 2$  for  $i = r_1 + 1, \dots, r_1 + r_2$ , and define for each  $x \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ , the norm function  $N(x) = \prod_{i=1}^{r_1+r_2} |x_i|^{e_i}$ , which corresponds to the absolute value of the norm on  $K$ , after the Minkowski embedding.

Given a choice of signs  $\vec{\eta} = (\eta_1, \dots, \eta_{r_1}) \in \{\pm 1\}^{r_1}$ , define the open orthant  $\mathbb{R}_{\vec{\eta}}^{r_1} = \{(x_1, \dots, x_{r_1}) \in \mathbb{R}^{r_1} \mid \text{sgn}(x_i) = \eta_i\}$ .

Since we are dealing with explicit results that take all constants into account, we will use the practical notation  $f = O^*(g)$  which means that  $|f| \leq g$ .

### 3. COUNTING LATTICE POINTS

We will count integral elements by embedding them in the Minkowski space as a (translate of a) lattice. We recall some definitions. Let  $S$  be a subset of  $\mathbb{R}^n$ , where we assume that  $n \geq 2$ . We say that  $S$  is of Lipschitz class  $\mathcal{L}(n, M, L)$  if there are  $M$  maps  $\phi_1, \dots, \phi_M : [0, 1]^{n-1} \rightarrow \mathbb{R}^n$  such that  $S$  is covered by the images of the maps  $\phi_i$ , and the maps satisfy the Lipschitz condition

$$(3) \quad \|\phi_i(x) - \phi_i(y)\| \leq L\|x - y\| \text{ for } x, y \in [0, 1]^{n-1}, i = 1, \dots, M.$$

We define the successive minima  $\lambda_i, i = 1, \dots, n$  of a lattice  $\Gamma$  as

$$\lambda_i = \inf\{\lambda \in \mathbb{R} \mid B(0, \lambda) \cap \Gamma \text{ contains } i \text{ linearly independent vectors}\}.$$

We define the orthogonality defect  $\Omega$  of a lattice  $\Gamma$  as

$$\Omega = \inf_{(v_1, \dots, v_n)} \frac{|v_1| \dots |v_n|}{\det \Gamma},$$

where the infimum runs over all bases  $(v_1, \dots, v_n)$  of  $\Gamma$ .

In order to count lattice points, we will use the following theorem by Widmer [23, Theorem 5.4]. The virtue of this theorem is that it is optimal in the successive minima and explicit in terms of the Lipschitz constant  $L$  and the dimension  $n$ .

**Lemma 3.** (Widmer) *Let  $\Gamma$  be a lattice in  $\mathbb{R}^n$  with successive minima  $\lambda_1, \dots, \lambda_n$  and orthogonality defect  $\Omega$ . Let  $S$  be a bounded set in  $\mathbb{R}^n$  such that the boundary*

$\partial S$  is of Lipschitz class  $\mathcal{L}(n, M, L)$ . Then  $S$  is measurable, and moreover,

$$\left| |S \cap \Gamma| - \frac{\text{Vol}(S)}{\det \Gamma} \right| \leq M(2\sqrt{n}\Omega + 4)^n \max_{0 \leq i < n} \frac{L^i}{\lambda_1 \dots \lambda_i},$$

or, since unconditionally we have  $\Omega \leq \frac{n^{\frac{3}{2}n}}{(2\pi)^{\frac{n}{2}}}$ ,

$$\left| |S \cap \Gamma| - \frac{\text{Vol}(S)}{\det \Gamma} \right| \leq Mn^{3n^2/2} \max_{0 \leq i < n} \frac{L^i}{\lambda_1 \dots \lambda_i},$$

*Remark.* We point out that the same result holds for translates of lattices. Indeed,  $|S \cap (\Gamma + v)| = |(S - v) \cap \Gamma|$ , and  $S - v$  is of the same Lipschitz class as  $S$ , and obviously has the same volume.

**3.1. Fundamental domain.** We now recall the fundamental domain under the action of multiplication by the fundamental units. For full details we refer the reader to [10]. Let

$$\begin{aligned} f : \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} &\rightarrow \mathbb{R}^{r+1} \\ (x_1, \dots, x_{r_1+r_2}) &\mapsto (\xi, \xi_1, \dots, \xi_r), \end{aligned}$$

where  $\xi$  and the  $\xi_j$  are defined by

$$(4) \quad \log(|x_i|) = \frac{\log(\xi)}{n} + \sum_{j=1}^r \xi_j \log(|\sigma_i(\varepsilon_j)|), \quad i = 1, \dots, r_1 + r_2,$$

or in other words,

$$(5) \quad |x_i| = \xi^{1/n} \prod_{j=1}^r |\sigma_i(\varepsilon_j)|^{\xi_j}, \quad i = 1, \dots, r_1 + r_2.$$

Note that since the units have norm one, it follows that  $\xi = |N(x)|$ .

The fundamental domain is then defined as  $\mathcal{F} = f^{-1}(\mathbb{R}_+ \times [0, 1)^r)$ . We remark that in what follows, we will always assume that  $K \neq \mathbb{Q}$ , since the results are trivial in this case. In the case that  $K$  is an imaginary quadratic field,  $r = 0$ , and in order for the proofs to remain valid, one should interpret the “empty product”  $\prod_{j=1}^r m_j$ , as well as the “empty determinant”  $\text{Reg}_K$ , as having the value 1.

We summarise a number of well-known facts in the following proposition

**Proposition 4.** *Consider the action of the non-torsion unit group  $U_K$  on Minkowski space  $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$  by multiplication. The set  $\mathcal{F}$  is a fundamental domain for this action. It is a cone, and defining*

$$\mathcal{F}(a_1, b_1, \dots, a_r, b_r; X) = f^{-1} \left( (0, X] \times \prod_{j=1}^r [a_j, b_j) \right),$$

we have that

$$\begin{aligned} \text{Vol}(\mathcal{F}(a_1, b_1, \dots, a_r, b_r; X)) &= X \prod_{j=1}^r (b_j - a_j) \text{Vol}(\mathcal{F}(0, 1, \dots, 0, 1; 1)) \\ (6) \quad &= X \prod_{j=1}^r (b_j - a_j) 2^{r_1} \pi^{r_2} \text{Reg}_K. \end{aligned}$$

We will denote some refinements of the fundamental domain in the following way.

$$\begin{aligned}\mathcal{F}_{\frac{1}{2}}(a_1, b_1, \dots, a_r, b_r; X) &= f^{-1} \left( \left( \frac{1}{2}X, X \right] \times \prod_{j=1}^r [a_j, b_j) \right), \\ \mathcal{F}_{\vec{\eta}}(a_1, b_1, \dots, a_r, b_r; X) &= \mathcal{F}(a_1, b_1, \dots, a_r, b_r; X) \cap \left( \mathbb{R}_{\vec{\eta}}^{r_1} \times \mathbb{C}^{r_2} \right), \\ \mathcal{F}_{\frac{1}{2}, \vec{\eta}}(a_1, b_1, \dots, a_r, b_r; X) &= \mathcal{F}_{\frac{1}{2}}(a_1, b_1, \dots, a_r, b_r; X) \cap \left( \mathbb{R}_{\vec{\eta}}^{r_1} \times \mathbb{C}^{r_2} \right).\end{aligned}$$

Finally,  $\mathcal{F}(X) = \mathcal{F}(0, 1, \dots, 0, 1; X)$ , and similarly for when the subscripts  $\frac{1}{2}$  or  $\vec{\eta}$  are present.

**3.2. A Partition of the fundamental domain.** We will be counting points in the fundamental domain  $\mathcal{F}$  using Lemma 3, with an explicit error term in terms of the Lipschitz constant. In order to optimize this process, we will instead count points in a *smaller* variant of the fundamental domain with a more regular shape. This trick was first used by Schmidt in [20] in the context of real quadratic fields, but has been applied in more general settings by Widmer [23], Gao [4]. The reason why we go through this partition step is because the Lipschitz constant of  $\mathcal{F}_{\frac{1}{2}, \vec{\eta}}(0, \frac{1}{m_1}, \dots, 0, \frac{1}{m_r}; X)$  is essentially independent of  $K$ , whereas the Lipschitz constant of  $\mathcal{F}_{\frac{1}{2}, \vec{\eta}}(X)$  is exponential in the  $m_j$ . Schmidt's partition trick will thus immediately reduce the dependence on the size of the logarithms of the fundamental units from an exponential dependence to a polynomial dependence.

**Lemma 5.** (*Schmidt's partition trick*) *Let  $\Gamma$  be a set of points in  $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ . Let  $\vec{k} \in \prod_{j=1}^r ([0, m_j) \cap \mathbb{Z})$  and denote  $\beta_{\vec{k}} = (\prod_{j=1}^r |\sigma_i(\varepsilon_j)|^{-k_j/m_j}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ , so that  $N(\beta_{\vec{k}}) = 1$ . Then*

$$|\Gamma \cap \mathcal{F}_{\frac{1}{2}, \vec{\eta}}(X)| = \sum_{\vec{k}} |(\Gamma \cdot \beta_{\vec{k}}) \cap \mathcal{F}_{\frac{1}{2}, \vec{\eta}}(0, \frac{1}{m_1}, \dots, 0, \frac{1}{m_r}; X)|,$$

where the sum runs over  $\vec{k} \in \prod_{j=1}^r ([0, m_j) \cap \mathbb{Z})$ .

*Proof.* We split up the unit hypercube  $[0, 1)^r$  as a union of sets  $\prod_{j=1}^r [\frac{k_j}{m_j}, \frac{k_j+1}{m_j})$ , for  $0 \leq k_j \leq m_j - 1, j = 1, \dots, r$ , so that

$$|\Gamma \cap \mathcal{F}_{\frac{1}{2}, \vec{\eta}}(X)| = \sum_{\substack{(k_1, \dots, k_r) \\ 0 \leq k_j \leq m_j - 1}} |\Gamma \cap \mathcal{F}_{\frac{1}{2}, \vec{\eta}}(\frac{k_1}{m_1}, \frac{k_1+1}{m_1}, \dots, \frac{k_r}{m_r}, \frac{k_r+1}{m_r}; X)|.$$

In each summand we multiply the elements in the intersection componentwise with

$$\beta_{\vec{k}} = \left( \prod_{j=1}^r |\sigma_1(\varepsilon_j)|^{-k_j/m_j}, \dots, \prod_{j=1}^r |\sigma_{r_1+r_2}(\varepsilon_j)|^{-k_j/m_j} \right),$$

a norm one element since  $\prod_{i=1}^{r_1+r_2} |\sigma_i(\varepsilon_j)|^{e_i} = 1$ . This gives a concrete bijection between the sets

$$\Gamma \cap \mathcal{F}_{\frac{1}{2}, \vec{\eta}}(\frac{k_1}{m_1}, \frac{k_1+1}{m_1}, \dots, \frac{k_r}{m_r}, \frac{k_r+1}{m_r}; X) = (\Gamma \cdot \beta_{\vec{k}}) \cap \mathcal{F}_{\frac{1}{2}, \vec{\eta}}(0, \frac{1}{m_1}, \dots, 0, \frac{1}{m_r}; X).$$

□

The following lemma will be practical in computing the Lipschitz constant of the fundamental domain.

**Lemma 6.** *Let  $f : \mathbb{R}^m \rightarrow \mathbb{R}$  be a function such that  $f(y_1, y_2, \dots, y_m) = c \prod_{j=1}^m g_j(y_j)$ , where the  $g_j : \mathbb{R} \rightarrow \mathbb{R}$  are functions that satisfy  $|g_j(y_j) - g_j(y'_j)| \leq K_j |y_j - y'_j|$  and  $|g_j(y_j)| \leq M_j$ . Then we have that*

$$(7) \quad |f(y_1, y_2, \dots, y_m) - f(y'_1, y'_2, \dots, y'_m)| \leq c \sum_{j=1}^m K_j \prod_{k \neq j} M_k \|y - y'\|.$$

Let  $h : \mathbb{R}^m \rightarrow \mathbb{R}^m, h = (h_1, \dots, h_m)$ , where the  $h_i : \mathbb{R}^m \rightarrow \mathbb{R}$  are functions that satisfy  $|h_i(y) - h_i(y')| \leq L_i \|y - y'\|$ . Then we have that

$$(8) \quad \|h(y) - h(y')\| \leq \sqrt{m} \max_i L_i \|y - y'\|$$

*Proof.* For the first inequality, let  $y^i = (y'_1, \dots, y'_i, y_{i+1}, \dots, y_m)$ . The result follows by writing the left hand side as  $|f(y) - f(y^1) + f(y^1) - f(y^2) + \dots - f(y^m)|$ , and the fact that  $|y_i - y'_i| \leq \|y - y'\|$ . The second inequality is obvious.  $\square$

**Lemma 7.** *The set  $\partial \mathcal{F}_{\frac{1}{2}, \bar{\eta}}(0, \frac{1}{m_1}, \dots, 0, \frac{1}{m_r}; t^n)$  is of Lipschitz-class  $\mathcal{L}(n, 2r + 2, Lt)$ , where*

$$L = (r + 2\pi)^{3/2} e^r.$$

*Proof.* We note that the Lipschitz constant of a blown-up set  $tR$  equals  $tL$ , where  $L$  is the Lipschitz constant of  $R$ , hence we can restrict attention to the case  $t = 1$ .

Note that for  $(x_1, \dots, x_{r_1+r_2}) \in \mathcal{F}_{\frac{1}{2}}(0, \frac{1}{m_1}, \dots, 0, \frac{1}{m_r}; 1)$ , by (4),  $\log(|x_i|)$  is bounded from below by some constant depending only on  $K$ . Hence the  $|x_i|$  are bounded away from zero, so that intersecting  $\mathcal{F}_{\frac{1}{2}}(0, \frac{1}{m_1}, \dots, 0, \frac{1}{m_r}; 1)$  with  $\mathbb{R}_{\bar{\eta}}^{r_1} \times \mathbb{C}^{r_2}$  does not create any additional boundary, that is,

$$\partial \mathcal{F}_{\frac{1}{2}, \bar{\eta}}(0, \frac{1}{m_1}, \dots, 0, \frac{1}{m_r}; 1) = \partial \mathcal{F}_{\frac{1}{2}}(0, \frac{1}{m_1}, \dots, 0, \frac{1}{m_r}; 1) \cap (\mathbb{R}_{\bar{\eta}}^{r_1} \times \mathbb{C}^{r_2}).$$

In order to cover  $\partial \mathcal{F}_{\frac{1}{2}, \bar{\eta}}(0, \frac{1}{m_1}, \dots, 0, \frac{1}{m_r}; 1)$  with the images of maps from  $[0, 1]^{n-1}$ , we consider the injective map

$$\begin{aligned} \tilde{f} : \mathbb{R}_{\bar{\eta}}^{r_1} \times \mathbb{C}^{r_2} &\rightarrow \mathbb{R}^n \\ (x_1, \dots, x_{r_1+r_2}) &\mapsto (f(x_1, \dots, x_{r_1+r_2}), \arg(x_{r_2+1}), \dots, \arg(x_{r_1+r_2})). \end{aligned}$$

Then

$$\begin{aligned} \partial \mathcal{F}_{\frac{1}{2}}(0, \frac{1}{m_1}, \dots, 0, \frac{1}{m_r}; 1) \cap (\mathbb{R}_{\bar{\eta}}^{r_1} \times \mathbb{C}^{r_2}) \\ = \partial f^{-1}\left(\left(\frac{1}{2}, 1\right] \times \prod_{j=1}^r \left[0, \frac{1}{m_j}\right)\right) \cap (\mathbb{R}_{\bar{\eta}}^{r_1} \times \mathbb{C}^{r_2}) \\ = \partial \tilde{f}^{-1}\left(\left(\frac{1}{2}, 1\right] \times \prod_{j=1}^r \left[0, \frac{1}{m_j}\right) \times [0, 2\pi)^{r_2}\right), \end{aligned}$$

and since  $\tilde{f}$  is continuous, we may conclude that

$$\partial \mathcal{F}_{\frac{1}{2}, \bar{\eta}}(0, \frac{1}{m_1}, \dots, 0, \frac{1}{m_r}; 1) = \tilde{f}^{-1} \partial \left( \left(\frac{1}{2}, 1\right] \times \prod_{j=1}^r \left[0, \frac{1}{m_j}\right) \times [0, 2\pi)^{r_2} \right),$$

so that  $\partial\mathcal{F}_{\frac{1}{2},\vec{\eta}}(0, \frac{1}{m_1}, \dots, 0, \frac{1}{m_r}; 1)$  is covered by the images of the  $2r+2$  maps  $\tilde{f}^{-1}$ , where one of the first  $r+1$  coordinates is fixed to be either  $\frac{1}{2}$  or 1, or 0 or  $\frac{1}{m_j}$ . Let us begin with the map fixing the first coordinate to be  $\frac{1}{2}$ :

$$\begin{aligned}\phi_1 : (y_1, \dots, y_{n-1}) &\mapsto \tilde{f}^{-1}\left(\frac{1}{2}, \frac{y_1}{m_1}, \dots, \frac{y_r}{m_r}, 2\pi y_{r+1}, \dots, 2\pi y_{n-1}\right) \\ &= (x_1, \dots, x_{r_1+r_2}),\end{aligned}$$

where

$$\begin{cases} x_i = \eta_i \left(\frac{1}{2}\right)^{1/n} \prod_{j=1}^r |\sigma_i(\varepsilon_j)|^{\frac{y_j}{m_j}} & \text{if } i \leq r_1, \\ x_i = e^{2\pi i y_i} \left(\frac{1}{2}\right)^{1/n} \prod_{j=1}^r |\sigma_i(\varepsilon_j)|^{\frac{y_j}{m_j}} & \text{if } r_1 < i \leq r_1 + r_2. \end{cases}$$

We will bound the Lipschitz constant of this map, using (8), by  $\sqrt{r_1 + r_2} \max_i L_i$ , where  $L_i$  is such that  $|x_i(y) - x_i(y')| \leq L_i \|y - y'\|$ . To bound  $L_i$ , we will use (7). Note that

$$\left| |\sigma_i(\varepsilon_j)|^{y_j/m_j} - |\sigma_i(\varepsilon_j)|^{y'_j/m_j} \right| \leq e |y_j - y'_j|, \quad \text{and} \quad |\sigma_i(\varepsilon_j)|^{y_j/m_j} \leq e,$$

from which it follows that in the case  $i \leq r_1$  we may take  $K_j = M_j = e$  for  $j \leq r$ ,  $K_j = 0, M_j = 1$  for  $j > r$ . Hence,  $L_i \leq (\frac{1}{2})^{1/n} r e^r$ . However, in the case  $r_1 < i \leq r_1 + r_2$ , we have  $K_i = 2\pi, M_i = 1$ , and all other  $K_j, M_j$  are as before. In this case  $L_i \leq (\frac{1}{2})^{1/n} (r e + 2\pi) e^{r-1}$ . Thus, the Lipschitz constant of this map  $\phi_1$  is bounded by  $(\frac{1}{2})^{1/n} \sqrt{r_1 + r_2} (r + 2\pi) e^r$ . Analogously, the map which fixed the first coordinate to be 1 instead of  $\frac{1}{2}$  has a Lipschitz constant which is bounded by  $\sqrt{r_1 + r_2} (r + 2\pi) e^r$ .

We use the same strategy to bound the Lipschitz constant of other maps  $\phi_k$  which fix the  $k$ 'th coefficient to be  $a \in \{0, \frac{1}{m_k}\}$ :

$$\begin{aligned}\phi_k : (y_0, \dots, \widehat{y_k}, \dots, y_{n-1}) &\mapsto \tilde{f}\left(\frac{1+y_0}{2}, \frac{y_1}{m_1}, \dots, a, \dots, \frac{y_r}{m_r}, 2\pi y_{r+1}, \dots, 2\pi y_{n-1}\right) \\ &= (x_1, \dots, x_{r_1+r_2}),\end{aligned}$$

where

$$\begin{cases} x_i = \eta_i \left(\frac{1+y_0}{2}\right)^{1/n} \prod_{\substack{j=1 \\ j \neq k}}^r |\sigma_i(\varepsilon_j)|^{\frac{y_j}{m_j}} |\sigma_i(\varepsilon_k)|^a & \text{if } i \leq r_1, \\ x_i = e^{2\pi i y_i} \left(\frac{1+y_0}{2}\right)^{1/n} \prod_{\substack{j=1 \\ j \neq k}}^r |\sigma_i(\varepsilon_j)|^{\frac{y_j}{m_j}} |\sigma_i(\varepsilon_k)|^a & \text{if } r_1 < i \leq r_1 + r_2. \end{cases}$$

We will bound the Lipschitz constant of this map, using (8), by  $\sqrt{r_1 + r_2} \max_i L_i$ , where  $L_i$  is such that  $|x_i(y) - x_i(y')| \leq L_i \|y - y'\|$ . To bound  $L_i$ , we will use (7). As with  $\phi_0$ , in the case  $i \leq r_1$  we may take  $K_j = M_j = e$  for  $1 \leq j \leq r$ ,  $K_j = 0, M_j = 1$  for  $j > r$ . Since

$$\left| \left(\frac{1+y_0}{2}\right)^{1/n} - \left(\frac{1+y'_0}{2}\right)^{1/n} \right| \leq \frac{1}{2^{1/n} n} |y_0 - y'_0|,$$



we may take  $K_0 = 1/n$  and  $M_0 = 1$ . Hence,  $L_i \leq |\sigma_i(\varepsilon_k)|^a (r-1+1/n)e^{r-1} \leq re^r$ . However, if  $r_1 < i \leq r_1 + r_2$ , we note that  $K_i = 2\pi, M_i = 1$ , and all other  $K_j, M_j$  are as before. In this case  $L_i \leq (r+2\pi)e^r$ . Thus, the Lipschitz constant of this map  $\phi_k$  is bounded by  $\sqrt{r_1 + r_2}(r+2\pi)e^r$ .  $\square$

We will need the following three lemmas.

**Lemma 8.** *Let  $x = (x_1, \dots, x_{r_1+r_2}) \in \mathcal{F}(0, \frac{1}{m_1}, \dots, 0, \frac{1}{m_r}; X)$ . Then*

$$\|x\| \leq \sqrt{r+1} e^r |N(x)|^{1/n}$$

*Proof.* This follows immediately from (5), the fact that  $\log |\sigma_i(\varepsilon_j)| \leq m_j$  and the inequality between the euclidean norm and the max-norm.  $\square$

We now fix our choice of fundamental units such that the product of the constants  $m_j$  approximates the regulator of the number field. This is possible by the following lemma.

**Lemma 9.** *There is a choice of fundamental units  $\varepsilon_1, \dots, \varepsilon_r$  such that*

$$\frac{1}{2^{r+1}(r+1)^{r/2}} \text{Reg}_K \leq \prod_{j=1}^r m_j \leq (2rn)^{2r} \text{Reg}_K.$$

*Proof.* Consider the logarithmic unit lattice  $\Lambda = \ell(\phi(U_K)) \in \mathbb{R}^{r+1}$  with  $\det \Lambda = \sqrt{r+1} \text{Reg}_K$ , where  $\ell(x_1, \dots, x_{r_1+r_2}) = (e_1 \log |x_1|, \dots, e_{r_1+r_2} \log |x_{r_1+r_2}|)$ . Since units have norm one, this lattice lies in the  $r$ -dimensional hyperplane  $x_1 + \dots + x_{r_1+r_2} = 0$ . The unconditional bound on the orthogonality defect implies that we can find a basis  $v_1, \dots, v_r$  of  $\Lambda$ , such that

$$(9) \quad 1 \leq \frac{\|v_1\| \dots \|v_r\|}{\det \Lambda} \leq \frac{r^{\frac{3}{2}r}}{(2\pi)^{\frac{r}{2}}}.$$

Now choose  $\varepsilon_j$  such that  $\ell(\phi(\varepsilon_j)) = v_j$ . Since the  $v_j$  form a basis, the  $\varepsilon_j$  form a set of fundamental units. For the lower bound, note that

$$m_j = \lceil \max_i (\log |\sigma_i(\varepsilon_j)|) \rceil \geq \frac{1}{2} \max_i (e_i \log |\sigma_i(\varepsilon_j)|) \geq \frac{1}{2\sqrt{r+1}} \|v_j\|,$$

and combine this with (9). For the upper bound, the case  $n = 2$  can be checked in an elementary way. For  $n \geq 3$ , note that by a theorem of Dobrowolski [2], we have that  $\max_i |\sigma_i(\varepsilon_j)| \geq 1 + \frac{\log n}{6n^2}$ , and hence  $\max_i \log |\sigma_i(\varepsilon_j)| \geq \frac{1}{7n^2}$ . This implies that

$$m_j \leq 7n^2 \max_i (e_i \log |\sigma_i(\varepsilon_j)|) \leq 7n^2 \|v_j\|,$$

which gives the upper bound when combined with (9).  $\square$

**Lemma 10.**

$$\int_{\mathbb{R}^r} \frac{dx_1 \dots dx_r}{\max_{1 \leq i \leq r+1} (\prod_{j=1}^r |\sigma_i(\varepsilon_j)|^{x_j/m_j} |\sigma_i(\alpha)|)^{n-1}} = \frac{1}{|N(\alpha)|^{\frac{n-1}{n}}} \frac{m_1 \dots m_r}{\text{Reg}_K} \left( \frac{n}{n-1} \right)^r$$

*Proof.* We start with the coordinate transformation  $x_j \mapsto x_j/m_j$ . Then, introducing the coordinate transformation  $y_i = \sum_{j=1}^r \log |\sigma_i(\varepsilon_j)| x_j$ ,  $i = 1, \dots, r$ , with determinant  $\prod_{i=1}^r e_i \frac{1}{\text{Reg}_K}$ , the integral equals

$$\prod_{i=1}^r e_i \frac{m_1 \dots m_r}{\text{Reg}_K} \int_{\mathbb{R}^r} \frac{dy_1 \dots dy_r}{\max(e^{y_1} |\sigma_1(\alpha)|, \dots, e^{y_r} |\sigma_r(\alpha)|, e^{-Y} |\sigma_{r+1}(\alpha)|)^{n-1}},$$

where  $Y = \frac{1}{e_{r+1}} \sum_{j=1}^r e_j y_j$ . We now apply the translation  $y_i \mapsto y_i + \log |\sigma_i(\alpha)| - \frac{\log |N(\alpha)|}{n}$  which allows us to pull out the factor  $|N(\alpha)|^{\frac{n-1}{n}}$ , and the integral equals

$$\prod_{i=1}^r e_i \frac{m_1 \dots m_r}{\text{Reg}_K |N(\alpha)|^{\frac{n-1}{n}}} \int_{\mathbb{R}^r} \frac{dy_1 \dots dy_r}{\max(e^{y_1}, \dots, e^{y_r}, e^{-Y})^{n-1}}.$$

Next, we introduce new coordinates  $z_1, \dots, z_r$  such that  $(n-1)y_i = nz_i - Z$ , where  $Z = \sum_{i=1}^r e_i z_i$ . We compute the determinant of this coordinate transformation, using the matrix determinant Lemma:

$$\begin{aligned} & \frac{1}{(n-1)^r} \det(nI - (e_1, \dots, e_r)^T(1, \dots, 1)) \\ &= \frac{1}{(n-1)^r} \det(nI) \left(1 - (1, \dots, 1) \left(\frac{1}{n} I\right) (e_1, \dots, e_r)^T\right) \\ &= e_r \frac{n^{r-1}}{(n-1)^r}. \end{aligned}$$

Noting that

$$(n-1)Y = \frac{n-1}{e_{r+1}} \sum_{i=1}^r e_i y_i = \frac{n}{e_{r+1}} Z - \frac{1}{e_{r+1}} \sum_{i=1}^r e_i Z = Z,$$

the integral equals

$$\prod_{i=1}^{r+1} e_i \frac{n^{r-1}}{(n-1)^r} \frac{m_1 \dots m_r}{\text{Reg}_K |N(\alpha)|^{\frac{n-1}{n}}} I,$$

where

$$I = \int_{\mathbb{R}^r} \frac{dz_1 \dots dz_r}{\max(e^{nz_1-Z}, \dots, e^{nz_r-Z}, e^{-Z})}.$$

Now let  $R_k = \{(z_1, \dots, z_r) \in \mathbb{R}^r \mid z_k > \max(0, z_1, \dots, z_r)\}$ . In this region, the integral equals

$$\begin{aligned} \int_{R_k} \frac{dz_1 \dots dz_r}{e^{nz_k-Z}} &= \int_{z_k \geq 0} \frac{dz_k}{e^{(n-e_k)z_k}} \prod_{\substack{i=1 \\ i \neq k}}^r \int_{z_i \leq z_k} \frac{dz_i}{e^{-e_i z_i}} \\ &= \int_{z_k \geq 0} \frac{dz_k}{e^{(n-e_k)z_k}} \prod_{\substack{i=1 \\ i \neq k}}^r \frac{1}{e^{-e_i z_k} e_i} \\ &= \prod_{\substack{i=1 \\ i \neq k}}^r \frac{1}{e_i} \int_0^\infty \frac{dz_k}{e^{e_{r+1} z_k}} = \prod_{\substack{i=1 \\ i \neq k}}^{r+1} \frac{1}{e_i}, \end{aligned}$$

while in the region  $S = \{(z_1, \dots, z_r) \in \mathbb{R}^r \mid z_i < 0, \forall i\}$ , the integral equals

$$\int_{z_i < 0 \forall i} \frac{dz_1 \dots dz_r}{e^{-Z}} = \prod_{i=1}^r \int_0^\infty \frac{dz_i}{e^{e_i z_i}} = \prod_{i=1}^r \frac{1}{e_i}.$$

Now  $\mathbb{R}^r$  is the disjoint union of the  $R_k$  and the set  $S$ , up to sets of measure zero, hence, the full integral  $I$  equals  $\frac{\sum_{i=1}^{r+1} e_i}{\prod_{i=1}^{r+1} e_i} = \frac{n}{\prod_{i=1}^{r+1} e_i}$ , and the result follows.  $\square$

**3.3. The counting theorem.** We are now ready to prove our key result counting elements of bounded norm in congruence classes modulo ideals in rings of integers, with given signs under the real embeddings, up to multiplication by units of infinite order. Let  $\mathfrak{C}$  be an ideal class, and let  $\mathfrak{b}_1, \mathfrak{b}_2, \dots$  be the integral ideals in  $\mathfrak{C}$  ordered such that  $N(\mathfrak{b}_1) \leq N(\mathfrak{b}_2) \leq \dots$ . Define

$$\mathfrak{N}(\mathfrak{C}) = \sum_{i=1}^{m_1 \dots m_r} \frac{1}{N(\mathfrak{b}_i)^{\frac{n-1}{n}}}.$$

**Theorem 11.** *Let  $\mathfrak{a}, \mathfrak{f}$  be coprime integral ideals of the ring of integers  $\mathcal{O}_K$  of a number field  $K$  of degree  $n$ . Let  $f \in \mathcal{O}_K$ , let  $\vec{\eta} \in \{\pm\}^{r_1}$ , and let  $\mathfrak{C}$  be the ideal class of  $\mathfrak{a}$ . Then*

$$\left| \left\{ \alpha \in \mathfrak{a} \left| \begin{array}{l} \phi(\alpha) \in \mathcal{F}_{\vec{\eta}}(t^n) \\ \alpha \equiv f \pmod{\mathfrak{f}} \end{array} \right. \right\} \right| = \frac{(2\pi)^{r_2} \text{Reg}_K}{\sqrt{|\Delta_K|} N(\mathfrak{a}\mathfrak{f})} t^n + O^* \left( n^{\frac{3}{2}n^2} e^{4n^2} \mathfrak{N}(\mathfrak{C}^{-1}) \frac{t^{n-1}}{N(\mathfrak{a})^{\frac{n-1}{n}}} \right),$$

*Proof.* We shall prove that

$$\left| \left\{ \alpha \in \mathfrak{a} \left| \begin{array}{l} \phi(\alpha) \in \mathcal{F}_{\frac{1}{2}, \vec{\eta}}(t^n) \\ \alpha \equiv f \pmod{\mathfrak{f}} \end{array} \right. \right\} \right| = \frac{(2\pi)^{r_2} \text{Reg}_K}{\sqrt{|\Delta_K|} N(\mathfrak{a}\mathfrak{f})} \frac{t^n}{2} + O^* \left( \frac{n^{\frac{3}{2}n^2} e^{4n^2}}{2} \mathfrak{N}(\mathfrak{C}^{-1}) \frac{t^{n-1}}{N(\mathfrak{a})^{\frac{n-1}{n}}} \right),$$

from which the statement follows by a dyadic summation.

Since  $\mathfrak{a}$  and  $\mathfrak{f}$  are coprime, we may choose  $f$  to be an element of  $\mathfrak{a}$  without changing its residue class mod  $\mathfrak{f}$ . The left hand side then equals

$$\left| (\phi(\mathfrak{a}\mathfrak{f}) + \phi(f)) \cap \mathcal{F}_{\frac{1}{2}, \vec{\eta}}(t^n) \right|.$$

We use Schmidt's partition trick, Lemma 5, to write the left hand side as

$$(10) \quad \sum_{\vec{k}} \left| (\phi(\mathfrak{a}\mathfrak{f}) + \phi(f)) \cdot \beta_{\vec{k}} \cap \mathcal{F}_{\frac{1}{2}, \vec{\eta}} \left( 0, \frac{1}{m_1}, \dots, 0, \frac{1}{m_r}; t^n \right) \right|.$$

We estimate each summand using Lemma 3, since by the remark after the theorem, the estimate holds whether or not the translation by  $\phi(f) \cdot \beta_{\vec{k}}$  is present. We consider the main term first,

$$\frac{\text{Vol}(\mathcal{F}_{\frac{1}{2}, \vec{\eta}}(0, \frac{1}{m_1}, \dots, 0, \frac{1}{m_r}; t^n))}{\det(\phi(\mathfrak{a}\mathfrak{f}) \cdot \beta_{\vec{k}})}.$$

Since  $\beta_{\vec{k}}$  is of norm one, the transformation is unimodular, and a standard computation gives

$$\det(\phi(\mathfrak{a}\mathfrak{f}) \cdot \beta_{\vec{k}}) = \det(\phi(\mathfrak{a}\mathfrak{f})) = 2^{-r_2} \sqrt{|\Delta_K|} N(\mathfrak{a}\mathfrak{f}).$$

Using (6) and the fact that  $\mathcal{F}$  is symmetric under reflection through the coordinate hyperplanes in the first  $r_1$  coordinates, we see that

$$\text{Vol}(\mathcal{F}_{\frac{1}{2}, \vec{\eta}}(0, \frac{1}{m_1}, \dots, 0, \frac{1}{m_r}; t^n)) = \frac{1}{2^{r_1}} \frac{2^{r_1} \pi^{r_2} \text{Reg}_K}{m_1 \dots m_r} \frac{t^n}{2},$$

so that the main term in each summand equals

$$\frac{1}{m_1 \dots m_r} \frac{(2\pi)^{r_2} \text{Reg}_K}{\sqrt{|\Delta_K|} N(\mathfrak{a}\mathfrak{f})} \frac{t^n}{2},$$

which yields the main term in the statement of the Lemma after summation over  $\vec{k} \in \prod_{j=1}^r [0, m_j) \cap \mathbb{Z}$ .

We now consider the error term. Since  $\mathcal{F}_{\frac{1}{2}, \vec{\eta}}(0, \frac{1}{m_1}, \dots, 0, \frac{1}{m_r}; t^n)$  is in Lipschitz class  $\mathcal{L}(n, 2r+2, Lt)$ , where  $L = (r+2\pi)^{3/2}e^r$ , the error term in estimating each summand is bounded by

$$(2r+2)n^{3n^2/2} \max_{0 \leq i \leq n-1} \frac{L^i t^i}{\lambda_1(\mathbf{a}, \vec{k}) \dots \lambda_i(\mathbf{a}, \vec{k})} \leq (2r+2)n^{3n^2/2} \max_{0 \leq i \leq n-1} \left( \frac{Lt}{\lambda_1(\mathbf{a}, \vec{k})} \right)^i,$$

where  $\lambda_i(\mathbf{a}, \vec{k})$  and  $\lambda_i(\mathbf{a}, \vec{k})$  are the successive minima of the lattices  $\phi(\mathbf{a}) \cdot \beta_{\vec{k}}$  and  $\phi(\mathbf{a}) \cdot \beta_{\vec{k}}$ , respectively.

We now claim that we may replace this maximum by setting  $i = n-1$ . This is certainly the case if  $\lambda_1(\mathbf{a}, \vec{k}) \leq Lt$ . The reason why we can do the same for those  $\vec{k}$  such that  $\lambda_1(\mathbf{a}, \vec{k}) > Lt$ , is that for these  $\vec{k}$ , the corresponding summand in (10) is zero, and moreover, the main term is bounded by the error term with the maximum replaced by setting  $i = n-1$ .

To prove that the summand is zero, consider a hypothetical element  $x$  in the intersection of  $(\phi(\mathbf{a}) + \phi(f)) \cdot \beta_{\vec{k}}$  and  $\mathcal{F}_{\frac{1}{2}, \vec{\eta}}(0, \frac{1}{m_1}, \dots, 0, \frac{1}{m_r}; t^n)$ . By Lemma 8 we have that  $\|x\| \leq \sqrt{r+1}e^r t$ , but since  $f \in \mathbf{a}$ , also  $\|x\| \geq \lambda_1(\mathbf{a}, \vec{k}) > Lt$ , which is a contradiction. Hence the summand is zero. Now we prove that the main term is smaller than the error term, or more precisely, that

$$(11) \quad \frac{1}{m_1 \dots m_r} \frac{(2\pi)^{r_2} \text{Reg}_K}{\sqrt{|\Delta_K|} N(\mathbf{a})} \frac{t^n}{2} \leq (2r+2)n^{3n^2/2} \frac{L^{n-1} t^{n-1}}{\lambda_1(\mathbf{a}, \vec{k})^{n-1}}.$$

We may multiply the right hand side with the factor  $\frac{Lt}{\lambda_1(\mathbf{a}, \vec{k})} < 1$ . By Minkowski's second theorem we have that  $\lambda_1(\mathbf{a}, \vec{k})^n \leq \frac{2^n}{\pi^{n/2}} \Gamma(1 + \frac{n}{2}) \det \phi(\mathbf{a}, \beta_{\vec{k}}) = \frac{2^n}{\pi^{n/2}} \Gamma(1 + \frac{n}{2}) 2^{-r_2} \sqrt{|\Delta_K|} N(\mathbf{a})$ , and by Lemma 9 we have that  $\text{Reg}_K \leq 2^{r+1}(r+1)^{r/2} m_1 \dots m_r$ , so after plugging in these inequalities, (11) follows from the inequality

$$\pi^{r_2} \frac{1}{2N(\mathbf{f})} \frac{2^n}{\pi^{n/2}} \Gamma(1 + \frac{n}{2}) 2^{r+1}(r+1)^{r/2} \leq (2r+2)n^{3n^2/2} L^n.$$

Hence, the total error term is bounded by

$$(12) \quad (2r+2)n^{3n^2/2} L^{n-1} t^{n-1} \sum_{\vec{k}} \frac{1}{\lambda_1(\mathbf{a}, \vec{k})^{n-1}}.$$

The last part of the proof is to bound the sum over  $\vec{k}$ . Define

$$\mu(\mathbf{a}, \vec{k}) = \min_{\alpha \in \mathbf{a}} \max_i (|\sigma_i(\alpha)| \prod_{j=1}^r |\sigma_i(\varepsilon_j)|^{-k_j/m_j}),$$

and note that  $\lambda_1(\mathbf{a}, \vec{k}) \geq \mu(\mathbf{a}, \vec{k})$ . For each element  $\alpha$ , define  $K_\alpha$  as the set of  $\vec{k} \in \prod_{j=1}^r [0, m_j) \cap \mathbb{Z}$  such that  $\alpha$  attains the minimal value in the definition of

$\mu(\mathfrak{a}, \vec{k})$ . We change the order in the sum

$$\begin{aligned} \sum_{\vec{k}} \frac{1}{\lambda_1(\mathfrak{a}, \vec{k})^{n-1}} &\leq \sum_{\vec{k}} \frac{1}{\mu(\mathfrak{a}, \vec{k})^{n-1}} \\ &\leq \sum'_{\alpha \in \mathfrak{a}} \sum_{u \in U_K} \sum_{\vec{k} \in K_{u\alpha}} \frac{1}{\max_i (|\sigma_i(u\alpha)| \prod_{j=1}^r |\sigma_i(\varepsilon_j)|^{-k_j/m_j})^{n-1}} \\ &\leq \sum'_{\alpha \in \mathfrak{a}} \sum_{\vec{k} \in \mathbb{Z}^r} \frac{1}{\max_i (|\sigma_i(\alpha)| \prod_{j=1}^r |\sigma_i(\varepsilon_j)|^{-k_j/m_j})^{n-1}}, \end{aligned}$$

where the dash signifies that the sum runs over pairwise non-associated elements  $\alpha$ , and the number of summands is at most  $m_1 \dots m_r$ .

We denote by  $g(\vec{k})$  the function in the last sum above. For any  $\vec{\delta} \in [0, 1]^r$ , we see that  $g(\vec{k}) \leq (e^r)^{n-1} g(\vec{k} + \vec{\delta})$ , and hence

$$\sum_{\vec{k} \in \mathbb{Z}^r} g(\vec{k}) \leq e^{r(n-1)} \int_{\vec{k} \in \mathbb{R}^r} g(\vec{k}) dk_1 \dots dk_r.$$

By Lemma 10, the sum is then bounded

$$\sum_{\vec{k}} \frac{1}{\lambda_1(\mathfrak{a}, \vec{k})^{n-1}} \leq e^{rn} \frac{m_1 \dots m_r}{\text{Reg}_K} \sum'_{\alpha \in \mathfrak{a}} \frac{1}{|N(\alpha)|^{\frac{n-1}{n}}}.$$

Since the elements  $\alpha \in \mathfrak{a}$ , it follows that  $(\alpha) = \mathfrak{a}\mathfrak{b}$ , for a certain  $\mathfrak{b} \in \mathfrak{C}^{-1}$ . Since the  $\alpha$  appearing in the sum are non-associated, all respective ideals  $\mathfrak{b}$  are different. Hence

$$\sum'_{\alpha \in \mathfrak{a}} \frac{1}{|N(\alpha)|^{\frac{n-1}{n}}} \leq \frac{1}{N(\mathfrak{a})^{\frac{n-1}{n}}} \mathfrak{N}(\mathfrak{C}^{-1}).$$

Gathering all this into (12), we see that the total error is bounded by

$$(2r+2)n^{3n^2/2} L^{n-1} e^{rn} \frac{m_1 \dots m_r}{\text{Reg}_K} \frac{t^{n-1}}{N(\mathfrak{a})^{\frac{n-1}{n}}} \mathfrak{N}(\mathfrak{C}^{-1}).$$

Using Lemma 9 to bound  $m_1 \dots m_r \leq (2rn)^{2r} \text{Reg}_K$ , and plugging in  $L = \sqrt{n}(r + 2\pi)e^r$ , the final step is to check that

$$(2r+2)n^{3n^2/2} ((r+2\pi)^{3/2} e^r)^{n-1} e^{rn} (2rn)^{2r} \leq n^{3n^2/2} \frac{e^{4n^2}}{2}. \quad \square$$

*Remark.* We give some comments on the error term. In terms of  $N(\mathfrak{a})$ , the result is best possible. The exponent of  $t$  might be improved, but would require an entirely different approach, as it is a consequence of our use of the Lipschitz-constant. In any case, any improvement of the exponent of  $t$  will naturally result to the same exponent in the successive minima  $\lambda_i$ , or thus in the power of  $N(\mathfrak{a})$ , which for our purposes would make little difference in the end. With regards to the field constants, we will see in Lemma 12 that  $\mathfrak{N}(\mathfrak{C}^{-1})$  is essentially  $\text{Reg}_K^{1/n}$ ; this substantial improvement over the linear dependence in the regulator that one gets by Schmidt's partition trick is the result of our careful analysis of the successive minima. In terms of the degree  $n$ , the main factor  $n^{3n^2/2}$  comes from Lemma 3, and with our approach, it can only be improved by finding a bound on the orthogonality defect of ideal lattices. As far as the author is aware, there is no reason to assume that ideal lattices have small orthogonality defect.

*Remark.* In the case  $\mathfrak{a} = \mathfrak{f} = \mathcal{O}_K$ , Theorem 11 is essentially (up to the quality of the constant in the error term) the same as the main result in [15], although we should mention that their proof is incomplete.

**Lemma 12.** *Let  $\mathfrak{b}_1, \mathfrak{b}_2, \dots$  be the integral ideals in  $\mathcal{O}_K$ , ordered such that  $N(\mathfrak{b}_1) \leq N(\mathfrak{b}_2) \leq \dots$ . Then, for all  $y \geq 3$ ,*

$$\sum_{i=1}^y \frac{1}{N(\mathfrak{b}_i)^{\frac{n-1}{n}}} \leq 6ny^{1/n} \log(y)^{\frac{(n-1)^2}{n}}.$$

*Proof.* Let  $m \in \mathbb{N}$ , then  $a_m$  will be largest in the case that all prime factors of  $m$  split completely. Then,

$$a_m \leq d_n(m),$$

where  $d_n(m)$  is the number of ways you can write  $m$  as a product of  $n$  integers. A result by Bordellès [1] gives the explicit upper bound

$$\sum_{1 \leq m \leq x} d_n(m) \leq 2x(\log x)^{n-1},$$

if  $x \geq 6$ . Hence,  $N(\mathfrak{b}_i) \geq \frac{i}{2(\log i)^{n-1}}$ , if the right hand side is at least 6. Hence, for all  $i \geq 3$ ,

$$N(\mathfrak{b}_i) \geq \frac{i}{6(\log i)^{n-1}}.$$

The result follows immediately.  $\square$

We can now easily deduce the explicit bound on the number of ideals of norm up to  $x$  stated in the introduction, hence making Landau's classical proof of the meromorphic continuation of  $\zeta_K(s)$  to  $\operatorname{Re}(s) > 1 - \frac{1}{n}$  explicit. Recall that  $\zeta_K(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ , where  $a_n$  is the number of ideals of norm  $n$ , and  $\kappa_K = \operatorname{res}_{s=1} \zeta_K(s)$ . We repeat the statement here for convenience.

**Corollary.** *Let  $K$  be a number field of degree  $n$ , and let  $a_k$  be the number of ideals of norm  $k$ . Then, for all  $x \geq 1$ ,*

$$\sum_{k \leq x} a_k = \kappa_K x + O^* \left( n^{10n^2} (\operatorname{Reg}_K h_K)^{1/n} (1 + \log \operatorname{Reg}_K h_K)^{\frac{(n-1)^2}{n}} x^{1-\frac{1}{n}} \right)$$

*Proof.* For each ideal class  $\mathfrak{C}$  we pick an integral ideal  $\mathfrak{b}$  in the inverse class  $\mathfrak{C}^{-1}$ . We then have a bijection between the set of integral ideals in  $\mathfrak{C}$  and the set of principal ideals in  $\mathfrak{b}$

$$\mathfrak{a} \mapsto \mathfrak{a}\mathfrak{b} = (\alpha),$$

with inverse  $(\alpha) \mapsto (\alpha)\mathfrak{b}^{-1}$ , which is an integral ideal since  $\mathfrak{b} | (\alpha)$ . Thus we may count the ideals  $\mathfrak{a}$  in the class  $\mathfrak{C}$  of norm up to  $x$  by counting the principal ideals inside  $\mathfrak{b}$  of norm up to  $xN(\mathfrak{b})$ . We do this by counting elements up to multiplication by units. If  $\omega$  is the number of roots of unity in  $K$ , we may write the number of all ideals in  $\mathfrak{C}$  of norm up to  $x$  as

$$\frac{1}{\omega} |\{\alpha \in \mathfrak{b} \mid \phi(\alpha) \in \mathcal{F}(xN(\mathfrak{b}))\}|.$$

Using the key lemma, we see that this equals

$$\frac{\kappa_K}{h_K N(\mathfrak{b})} xN(\mathfrak{b}) + O^* \left( 2^{r_1} n^{\frac{3}{2}n^2} e^{4n^2} \mathfrak{N}(\mathfrak{C}^{-1}) \frac{(N(\mathfrak{b})x)^{1-\frac{1}{n}}}{N(\mathfrak{b})^{\frac{n-1}{n}}} \right).$$

Summing over all ideal classes, we get

$$\sum_{m \leq x} a_m = \kappa x + O^* \left( 2^{r_1} n^{\frac{3}{2}n^2} e^{4n^2} \sum_{\mathfrak{c}} \mathfrak{N}(\mathfrak{c}^{-1}) x^{1-\frac{1}{n}} \right).$$

Using Lemma 12 with  $y = h_K m_1 \dots m_r \leq (2rn)^{2r} \text{Reg}_K h_K$ , the statement follows after checking that

$$2^{r_1} n^{\frac{3}{2}n^2} e^{4n^2} 6n(2rn)^{2r/n} (2r \log(2rn))^{\frac{(n-1)^2}{n}} \leq n^{10n^2}.$$

□

#### 4. THE SELBERG SIEVE IN RINGS OF INTEGERS

We will use the Selberg sieve in the ring of integers  $\mathcal{O}_K$ , or more precisely, in the arithmetic semigroup of the integral ideals. We note that in the literature, the phrase “Selberg sieve in rings of integers” has been used with another meaning (see [6], [17], [18] and [19]), namely the sifting of integral elements whose conjugates are restricted to lie in a box. This is a quite different story from our setup of working with ideals, which will amount to considering integral elements up to multiplication by units.

Concretely, let  $\mathcal{A}$  be a set of nonzero integral ideals in  $\mathcal{O}_K$ , let  $\mathcal{P}$  be a set of prime ideals in  $\mathcal{O}_K$ , and let  $\overline{\mathcal{P}}$  be the complement of  $\mathcal{P}$  in the set of prime ideals. The sifted set is defined, analogously to the case  $K = \mathbb{Q}$ , as

$$S(\mathcal{A}, \mathcal{P}, z) = \{\mathfrak{a} \in \mathcal{A} \mid (\mathfrak{a}, \mathcal{P}(z)) = 1\}, \quad \text{where} \quad \mathcal{P}(z) = \prod_{\substack{\mathfrak{p} \in \mathcal{P} \\ N(\mathfrak{p}) \leq z}} \mathfrak{p}.$$

In what follows,  $\mu$  will denote the Möbius function on the integral ideals,  $\nu$  is the function counting prime divisors, defined by  $\nu(\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_k^{e_k}) = \sum e_i$ , and  $\phi(\mathfrak{d}) = |(\mathcal{O}_K/\mathfrak{d})^*| = \prod_{\mathfrak{p} \mid \mathfrak{d}} N(\mathfrak{p}^{k-1})(N(\mathfrak{p}) - 1)$  is the generalisation of the euler totient. One may then completely transfer Chapter 3.1 in [5] to our situation, working with integral ideals instead of integers. In particular, the Selberg sieve weights are now a collection of reals  $\lambda_{\mathfrak{d}}$  where  $\mathfrak{d}$  ranges over the squarefree integral ideals. The only caveat is that all instances of integers in situations where its magnitude is the relevant property should be translated into the norms of the integral ideals. For completeness we give the definition of the relevant quantities. Let  $\omega$  be a multiplicative function on the integral ideals.

$$\begin{aligned} g(\mathfrak{d}) &= \frac{\omega(\mathfrak{d})}{N(\mathfrak{d}) \prod_{\mathfrak{p} \mid \mathfrak{d}} (1 - \frac{\omega(\mathfrak{p})}{N(\mathfrak{p})})} \\ G_{\mathfrak{k}}(x) &= \sum_{\substack{N(\mathfrak{d}) \leq x \\ (\mathfrak{d}, \mathfrak{k})=1}} \mu^2(\mathfrak{d}) g(\mathfrak{d}), \quad \text{and} \quad G(x) = G_{\mathcal{O}_K}(x) \\ \lambda_{\mathfrak{d}} &= \frac{\mu(\mathfrak{d})}{\prod_{\mathfrak{p} \mid \mathfrak{d}} (1 - \frac{\omega(\mathfrak{p})}{N(\mathfrak{p})})} \frac{G_{\mathfrak{d}}(z/N(\mathfrak{d}))}{G(z)} \end{aligned}$$

With this slightly generalised setup, Theorem 3.2 in [5] immediately generalises to the following Theorem.

**Theorem 13.** Assume that  $|\mathcal{A}_{\mathfrak{d}}| = \frac{\omega(\mathfrak{d})}{N(\mathfrak{d})}X + R_{\mathfrak{d}}$ , where  $\omega$  is a multiplicative function on the integral ideals in  $\mathcal{O}_K$  satisfying  $0 \leq \frac{\omega(\mathfrak{p})}{N(\mathfrak{p})} \leq 1 - \frac{1}{A}$  for some constant  $A$ . Then

$$S(\mathcal{A}, \mathcal{P}, z) \leq \frac{X}{G(z)} + \Sigma_2,$$

where

$$\Sigma_2 \leq \sum_{\substack{N(\mathfrak{d}_i) \leq z \\ \mathfrak{d}_i | \mathcal{P}(z) \\ i=1,2}} |R_{[\mathfrak{d}_1, \mathfrak{d}_2]}| \leq \sum_{\substack{N(\mathfrak{d}) < z^2 \\ \mathfrak{d} | \mathcal{P}(z)}} 3^{\nu(\mathfrak{d})} |R_{\mathfrak{d}}|.$$

In the case that  $\omega = 1$ , we can give a lower bound for  $G(z)$ .

**Lemma 14.** Let  $K$  be a number field of degree  $n$ . Let  $\omega(\mathfrak{p}) = 1, \forall \mathfrak{p} \in \mathcal{P}$ , and  $\omega(\mathfrak{p}) = 0, \forall \mathfrak{p} \in \overline{\mathcal{P}}$ . Let  $c = n^{10n^2} (\text{Reg}_K h_K)^{1/n} (1 + \log \text{Reg}_K h_K)^{\frac{(n-1)^2}{n}}$ . Then we have, for all  $z \geq (ec/\kappa_K)^n$ , that

$$G(z) \geq \prod_{\substack{\mathfrak{p} \in \overline{\mathcal{P}} \\ N(\mathfrak{p}) \leq z}} \left(1 - \frac{1}{N(\mathfrak{p})}\right) \kappa_K \log \left( \frac{\kappa_K^n z}{e^n c^n} \right).$$

*Proof.* Denote  $\mathfrak{m} = \prod_{\substack{\mathfrak{p} \in \overline{\mathcal{P}} \\ N(\mathfrak{p}) \leq z}} \mathfrak{p}$ . Then

$$G(z) = \sum_{\substack{N(\mathfrak{d}) < z \\ (\mathfrak{d}, \mathfrak{m})=1}} \frac{\mu^2(\mathfrak{d})}{\prod_{\mathfrak{p}|\mathfrak{d}} (N(\mathfrak{p}) - 1)} = \sum_{\substack{N(\mathfrak{d}) < z \\ (\mathfrak{d}, \mathfrak{m})=1}} \frac{\mu^2(\mathfrak{d})}{\phi(\mathfrak{d})}.$$

Note first that

$$\begin{aligned} G(z) \prod_{\substack{N(\mathfrak{q}) < z \\ \mathfrak{q}|\mathfrak{m}}} \left(1 - \frac{1}{N(\mathfrak{q})}\right)^{-1} &= \sum_{\substack{(\mathfrak{d}, \mathfrak{m})=1 \\ N(\mathfrak{d}) \leq z}} \frac{\mu^2(\mathfrak{d})}{\phi(\mathfrak{d})} \prod_{\substack{N(\mathfrak{q}) < z \\ \mathfrak{q}|\mathfrak{m}}} \left(1 - \frac{1}{N(\mathfrak{q})}\right)^{-1} \\ &= \sum_{\substack{(\mathfrak{d}, \mathfrak{m})=1 \\ N(\mathfrak{d}) \leq z}} \frac{\mu^2(\mathfrak{d})}{\phi(\mathfrak{d})} \prod_{\substack{N(\mathfrak{q}) < z \\ \mathfrak{q}|\mathfrak{m}}} \left(1 + \frac{1}{N(\mathfrak{q}) - 1}\right) \\ &\geq \sum_{N(\mathfrak{d}) \leq z} \frac{\mu^2(\mathfrak{d})}{\phi(\mathfrak{d})}. \end{aligned}$$

We may further reduce the sum

$$\sum_{N(\mathfrak{d}) \leq z} \frac{\mu^2(\mathfrak{d})}{\phi(\mathfrak{d})} = \sum_{N(\mathfrak{d}) \leq z} \frac{\mu^2(\mathfrak{d})}{N(\mathfrak{d})} \prod_{\mathfrak{p}|\mathfrak{d}} \left(1 - \frac{1}{N(\mathfrak{p})}\right)^{-1} \geq \sum_{N(\mathfrak{a}) \leq z} \frac{1}{N(\mathfrak{a})}.$$

Let  $S(x) = \sum_{m \leq x} a_m$ . By partial summation,

$$\begin{aligned} \sum_{m \leq z} \frac{a_m}{m} &= \sum_{m \leq y} \frac{a_m}{m} + \sum_{y \leq m \leq z-1} \frac{S(m)}{m(m+1)} + \frac{S(z-1)}{z-1} - \frac{S(y-1)}{y} \\ &\geq \kappa_K (\log(z) - \log(y+1)) - nc \frac{1}{(y+1)^{1/n}}, \end{aligned}$$

where we have used Theorem 2. Choosing  $y+1 = (c/\kappa_K)^n$  yields the theorem.  $\square$



The following lemma deals with the error term in the case that  $|R_{\mathfrak{d}}| \ll \frac{1}{N(\mathfrak{d})^{1-\frac{1}{n}}}$ .

**Lemma 15.** *Let  $K$  be a number field of degree  $n$ . Then, for all  $z \geq 16$ ,*

$$\sum_{\substack{N(\mathfrak{d}) \leq z^2 \\ \mathfrak{d} | \mathcal{P}(z)}} 3^{\nu(\mathfrak{d})} \frac{1}{N(\mathfrak{d})^{1-\frac{1}{n}}} \leq z^{2/n} (2 \log z)^{3n}.$$

*Proof.* Since a prime can split into at most  $n$  prime ideals  $\mathfrak{p}$  in  $\mathcal{O}_K$ , with norms at least  $p$ , we have that

$$\sum_{N(\mathfrak{p}) \leq z} \frac{1}{N(\mathfrak{p})} \leq n \sum_{p \leq z} \frac{1}{p}.$$

Since by [3],  $p_k \geq k(\log k + \log \log k - 1) \geq k \log k$  for  $k \geq e^e = 15, 154, \dots$ . Hence,

$$\sum_{p \leq z} \frac{1}{p} = \sum_{k \leq 15} \frac{1}{p_k} + \sum_{16 \leq k \leq z} \frac{1}{p_k} \leq 0,666 + \log \log z,$$

for  $z \geq 16$ . We may conclude that

$$(13) \quad \prod_{N(\mathfrak{p}) \leq z} \left(1 + \frac{1}{N(\mathfrak{p})}\right) \leq e^{\sum_{N(\mathfrak{p}) \leq z} \frac{1}{N(\mathfrak{p})}} \leq (2 \log z)^n,$$

since  $e^{0,666} \leq 2$ . Now note that

$$\begin{aligned} \sum_{\substack{N(\mathfrak{d}) \leq z^2 \\ \mathfrak{d} | \mathcal{P}(z)}} 3^{\nu(\mathfrak{d})} \frac{1}{N(\mathfrak{d})^{1-\frac{1}{n}}} &\leq z^{2/n} \sum_{\substack{N(\mathfrak{d}) \leq z^2 \\ \mathfrak{d} | \mathcal{P}(z)}} 3^{\nu(\mathfrak{d})} \frac{1}{N(\mathfrak{d})} \\ &\leq z^{2/n} \prod_{\substack{N(\mathfrak{p}) \leq z \\ \mathfrak{p} \in \mathcal{P}}} \left(1 + \frac{1}{N(\mathfrak{p})}\right)^3 \\ &\leq z^{2/n} (2 \log z)^{3n}. \end{aligned} \quad \square$$

## 5. ARTIN'S RECIPROCITY LAW AND PROOF OF THEOREM 1

Let  $\mathfrak{f}$  an integral ideal in  $\mathcal{O}_K$ . Recall the narrow class group to the modulus  $\mathfrak{f}$ , denoted by  $H_{\mathfrak{f}}^*$ . We will denote the order of this group by  $h_{\mathfrak{f}}^*$ . Consider the map

$$\begin{aligned} \rho : \{\alpha \in \mathcal{O}_K \mid (\alpha, \mathfrak{f}) = 1\} &\rightarrow (\mathcal{O}_K/\mathfrak{f})^* \times \{\pm 1\}^{r_1} \\ \alpha &\mapsto (\alpha + \mathfrak{f}, \text{sgn } \sigma_1(\alpha), \dots, \text{sgn } \sigma_{r_1}(\alpha)), \end{aligned}$$

and let  $V_K$  be the group of all units in  $\mathcal{O}_K$ , including roots of unity. Then  $(\alpha)$  is in the trivial class, denoted  $\mathfrak{e}$ , of  $H_{\mathfrak{f}}^*$  if and only if  $\rho(\alpha) \in \rho(V_K)$ , and we have that

$$h_{\mathfrak{f}}^* = \frac{2^{r_1} \phi(\mathfrak{f})}{|\rho(V_K)|} h_K,$$

moreover, each ideal class splits into

$$\frac{2^{r_1} \prod_{\mathfrak{p} | \mathfrak{f}} \left(1 - \frac{1}{N(\mathfrak{p})}\right) N(\mathfrak{f})}{|\rho(V_K)|}$$

narrow classes mod  $\mathfrak{f}$ . The narrow class groups mod  $\mathfrak{f}$  are relevant in Class Field Theory, and in the Artin reciprocity law in particular. One possible statement of Artin reciprocity law reads as follows (see [16, p. 389]).

**Theorem 16.** (*Artin Reciprocity Law*) *If  $L/K$  is Abelian and  $G$  is its Galois group, then there exists an ideal  $\mathfrak{f}$  in  $\mathcal{O}_K$  such that the prime ideals ramified under  $L/K$  coincide with the prime ideals dividing  $\mathfrak{f}$ , and if  $\mathfrak{p}_1$  and  $\mathfrak{p}_2$  are two unramified prime ideals in the same class in  $H_{\mathfrak{f}}^*$ , then  $\text{Frob}_{L/K}(\mathfrak{p}_1) = \text{Frob}_{L/K}(\mathfrak{p}_2)$ . The map of  $H_{\mathfrak{f}}^*$  into  $G$  induced in this way by  $\text{Frob}_{L/K}$  turns out to be a surjective homomorphism.*

The ideal  $\mathfrak{f}$  with smallest norm such that the above holds is called the conductor of  $L/K$ . The strategy to count primes with a given Frobenius conjugacy class  $C \subset \text{Gal}(L/\mathbb{Q})$  can then be outlined in the following steps.

- (a) Choose an abelian subgroup  $H \leq G$  such that  $C \cap H$  is nonempty. Let  $K$  be the subfield corresponding to  $H$ . We reduce to the problem of counting prime ideals in  $\mathcal{O}_K$  with a given Frobenius in the *abelian* extension  $L/K$ .
- (b) Applying the Artin reciprocity law, we reduce this to the problem of counting prime ideals in given narrow ideal classes mod  $\mathfrak{f}$ .
- (c) Using our explicit Selberg Sieve, this is reduced to the problem of counting ideals in given narrow ideal classes mod  $\mathfrak{f}$ , which is then achieved by means of our counting result, Theorem 11.

The following proposition gathers all parts of the proof of Theorem 1 which rely on the Selberg Sieve and the counting result, Theorem 11.

**Proposition 17.** *Let  $R$  be a subset of the narrow class group  $H_{\mathfrak{f}}^*$ . Let*

$$\mathcal{A} = \cup_{\mathfrak{c} \in R} \{ \mathfrak{a} \text{ integral ideal in } \mathcal{O}_K \mid \frac{N(\mathfrak{a})}{N(\mathfrak{c})} \leq x \},$$

*and let  $\mathcal{P}$  consist of all primes coprime to  $\mathfrak{f}$ . Let  $z \geq (ec/\kappa_K)^n$ . Then*

$$S(\mathcal{A}, \mathcal{P}, z) = \frac{R}{h_{\mathfrak{f}}^*} \frac{x}{\log \left( \frac{\kappa_K^n z}{e^n c^n} \right)} + N(\mathfrak{f}) c x^{1 - \frac{1}{n}} z^{\frac{2}{n}} (2 \log z)^{3n},$$

*where  $c = n^{10n^2} (\text{Reg}_K h_K)^{1/n} (1 + \log \text{Reg}_K h_K)^{\frac{(n-1)^2}{n}}$ .*

*Proof.* Let  $\mathfrak{d}$  be a squarefree ideal coprime with  $\mathfrak{f}$ , and consider the set  $\{ \mathfrak{a} \subset \mathfrak{d} \mid \mathfrak{a} \in \mathfrak{c}, N(\mathfrak{a}) \leq x \}$ . Choose an ideal  $\mathfrak{b} \in \mathfrak{c}^{-1}$ . Then, this set has cardinality equal to

$$\begin{aligned} & |\{ (\alpha) \subset \mathfrak{d}\mathfrak{b} \mid (\alpha) \in \mathfrak{c}, N(\alpha) \leq xN(\mathfrak{b}) \}| \\ &= \frac{1}{\omega} |\{ \alpha \in \mathfrak{d}\mathfrak{b} \mid \rho(\alpha) \in \rho(V_K), \alpha \in \mathcal{F}(xN(\mathfrak{b})) \}| \\ &= \frac{1}{\omega} \sum_{k=1}^{|\rho(V_K)|} |\{ \alpha \in \mathfrak{d}\mathfrak{b} \mid \alpha \equiv u_k \pmod{\mathfrak{f}}, \alpha \in \mathcal{F}_{(\text{sgn } \sigma_i(u_k))}(xN(\mathfrak{b})) \}|, \end{aligned}$$

where the  $u_k$  are such that  $\rho(V_K) = \{ \rho(u_k) \mid k = 1, \dots, |\rho(V_K)| \}$ . By Theorem 11, this is

$$\frac{|\rho(V_K)|}{\omega} \left( \frac{\omega \kappa_K}{2^{r_1} N(\mathfrak{f}) h_K} \frac{x}{N(\mathfrak{d})} + O^* \left( n^{\frac{3}{2}n^2} e^{4n^2} \mathfrak{N}(\mathfrak{C}) \frac{x^{\frac{n-1}{n}}}{N(\mathfrak{d})^{\frac{n-1}{n}}} \right) \right),$$

where  $\mathfrak{C}$  is the ideal class of  $(\mathfrak{b}\mathfrak{d})^{-1}$ . We sum this over  $R$  classes  $\mathfrak{c}$  to get an estimate for  $|\mathcal{A}_{\mathfrak{d}}|$ . As a main term we get

$$\frac{R \prod_{\mathfrak{p} \mid \mathfrak{f}} \left( 1 - \frac{1}{N(\mathfrak{p})} \right) \kappa_K}{h_{\mathfrak{f}}^*} \frac{x}{N(\mathfrak{d})}.$$

We bound the error term above by summing over all  $h_{\mathfrak{f}}^*$  classes, and we get

$$\begin{aligned} |R_{\mathfrak{d}}| &\leq \frac{2^{r_1} \prod_{\mathfrak{p}|\mathfrak{f}} \left(1 - \frac{1}{N(\mathfrak{p})}\right) N(\mathfrak{f})}{\omega} n^{\frac{3}{2}n^2} e^{4n^2} \left( \sum_{i=1}^{h_K m_1 \dots m_r} \frac{1}{N(\mathfrak{b})^{\frac{n-1}{n}}} \right) \frac{x^{\frac{n-1}{n}}}{N(\mathfrak{d})^{\frac{n-1}{n}}} \\ &\leq N(\mathfrak{f}) c \frac{x^{\frac{n-1}{n}}}{N(\mathfrak{d})^{\frac{n-1}{n}}}, \end{aligned}$$

by applying Lemma 12 in the same way as in the proof of Theorem 2. The statement now follows by applying Selberg's Sieve, Theorem 13, and Lemmata 14 and 15.  $\square$

*Proof of Theorem 1.* Let  $H \leq \text{Gal}(L/\mathbb{Q})$  be the maximal abelian subgroup such that  $H \cap C$  is non-empty. Let  $K$  be the fixed field of  $H$ , and choose  $c \in C \cap H$ . Let  $n$  be the degree of  $K$ . It is an exercise in basic algebraic number theory to prove that

$$\pi_C(x, L/\mathbb{Q}) \leq \frac{|C|}{n} |\{\mathfrak{p} \text{ unramified prime ideal in } \mathcal{O}_K \mid \text{Frob}_{L/K}(\mathfrak{p}) = c, N(\mathfrak{p}) \leq x\}|.$$

By the Artin reciprocity law, there is a subset  $R \subseteq H_{\mathfrak{f}}^*$  of size  $\frac{h_{\mathfrak{f}}^*}{[L:K]}$  such that

$$\pi_C(x, L/\mathbb{Q}) \leq \frac{|C|}{n} \sum_{\mathfrak{c} \in R} |\{\mathfrak{p} \text{ prime ideal in } \mathcal{O}_K \mid \mathfrak{p} \in \mathfrak{c}, N(\mathfrak{p}) \leq x\}|.$$

By Proposition 17, we may bound this by

$$\frac{|C|}{n} \left( \frac{1}{[L:K]} \frac{x}{\log\left(\frac{\kappa_K^n z}{e^n c^n}\right)} + N(\mathfrak{f}) c x^{1-\frac{1}{n}} z^{\frac{2}{n}} (2 \log z)^{3n} + n\pi(z) \right),$$

where  $c = n^{10n^2} (\text{Reg}_K h_K)^{1/n} (1 + \log \text{Reg}_K h_K)^{\frac{(n-1)^2}{n}}$ , for any  $z \geq (ec/\kappa_K)^n$ . We choose  $z^2 = \frac{x}{(\log x)^{4n^2} (c[L:K]N(\mathfrak{f}))^n}$ , which is a valid choice since  $\frac{x}{(\log x)^{5n^2}} \geq e^{2n} c^{3n} [L:K]^n N(\mathfrak{f})^n \frac{1}{\kappa_K^{2n}}$ . This choice of  $z$  makes sure that

$$N(\mathfrak{f}) c x^{1-\frac{1}{n}} z^{\frac{2}{n}} (2 \log z)^{3n} + n\pi(z) \leq \frac{x}{[L:K](\log x)^2},$$

while

$$\frac{x}{\log\left(\frac{\kappa_K^n z}{e^n c^n}\right)} \leq \frac{2x}{\log(x/c_K) - 4n^2 \log_2 x},$$

where  $c_K = n^{31n^3} (\text{Reg}_K h_K)^3 (1 + \log \text{Reg}_K h_K)^{3(n-1)^2} [L:K]^n N(\mathfrak{f})^n \kappa_K^{-2n}$ . Now

$$\begin{aligned} &\frac{1}{\log(x/c_K) - 4n^2 \log_2 x} \\ &= \frac{1}{\log(x/c_K)} + \frac{4n^2 \log_2 x}{\log(x/c_K)(\log(x/c_K) - 4n^2 \log_2 x)} \\ &\leq \frac{1}{\log(x/c_K)} + \frac{20n^2 \log_2 x}{\log(x/c_K)^2}, \end{aligned}$$

since  $(\log x)^{5n^2} \leq x/c_K$  by assumption. In conclusion, we have bounded  $\pi_C(x, L/\mathbb{Q})$  above by

$$\frac{|C|}{|G|} \left( \frac{2x}{\log(x/c_K)} + \frac{20n^2 \log_2 x}{\log(x/c_K)} \frac{2x}{\log(x/c_K)} + \frac{x}{(\log x)^2} \right). \quad \square$$

## REFERENCES

- [1] O. BORDELLÈS, *Explicit upper bounds for the average order of  $d_n(m)$  and application to class number*, JIPAM. J. Inequal. Pure Appl. Math., 3 (2002), pp. Article 38, 15 pp. (electronic).
- [2] E. DOBROWOLSKI, *On the maximal modulus of conjugates of an algebraic integer*, Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys., 26 (1978), pp. 291–292.
- [3] P. DUSART, *The  $k$ th prime is greater than  $k(\ln k + \ln \ln k - 1)$  for  $k \geq 2$* , Math. Comp., 68 (1999), pp. 411–415.
- [4] X. GAO, *On Northcott's Theorem*, PhD thesis, University of Colorado, 1995.
- [5] H. HALBERSTAM AND H.-E. RICHERT, *Sieve methods*, Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], London-New York, 1974. London Mathematical Society Monographs, No. 4.
- [6] J. G. HINZ, *An application of algebraic sieve theory*, Arch. Math. (Basel), 80 (2003), pp. 586–599.
- [7] R. M. KAUFMAN, *Estimate of the Hecke  $L$ -functions on the half line*, Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI), 91 (1979), pp. 40–51, 180–181. Analytic number theory and the theory of functions, 2.
- [8] J. C. LAGARIAS, H. L. MONTGOMERY, AND A. M. ODLYZKO, *A bound for the least prime ideal in the Chebotarev density theorem*, Invent. Math., 54 (1979), pp. 271–296.
- [9] J. C. LAGARIAS AND A. M. ODLYZKO, *Effective versions of the Chebotarev density theorem*, in Algebraic number fields:  $L$ -functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London, 1977, pp. 409–464.
- [10] S. LANG, *Algebraic number theory*, vol. 110 of Graduate Texts in Mathematics, Springer-Verlag, New York, second ed., 1994.
- [11] H. LAO, *On the distribution of integral ideals and Hecke Grössencharacters*, Chin. Ann. Math. Ser. B, 31 (2010), pp. 385–392.
- [12] S. LOUBOUTIN, *Explicit upper bounds for residues of Dedekind zeta functions and values of  $L$ -functions at  $s = 1$ , and explicit lower bounds for relative class numbers of CM-fields*, Canad. J. Math., 53 (2001), pp. 1194–1222.
- [13] J. MAYNARD, *On the Brun-Titchmarsh theorem*, Acta Arith., 157 (2013), pp. 249–296.
- [14] H. L. MONTGOMERY AND R. C. VAUGHAN, *The large sieve*, Mathematika, 20 (1973), pp. 119–134.
- [15] M. R. MURTY AND J. VAN ORDER, *Counting integral ideals in a number field*, Expo. Math., 25 (2007), pp. 53–66.
- [16] W. NARKIEWICZ, *Elementary and analytic theory of algebraic numbers*, Springer-Verlag Warszawa, Berlin, 1990.
- [17] G. J. RIEGER, *Verallgemeinerung der Siebmethode von A. Selberg auf Algebraische Zahlkörper. III*, J. Reine Angew. Math., 208 (1961), pp. 79–90.
- [18] H. SARGES, *Eine Anwendung des Selbergschen Siebes auf algebraische Zahlkörper*, Acta Arith., 28 (1975/76), pp. 433–455.
- [19] W. SCHAAL, *Obere und untere Abschätzungen in algebraischen Zahlkörpern mit Hilfe des linearen Selbergschen Siebes*, Acta Arith., 13 (1967/1968), pp. 267–313.
- [20] W. M. SCHMIDT, *Northcott's theorem on heights. II. The quadratic case*, Acta Arith., 70 (1995), pp. 343–375.
- [21] H. M. STARK, *Some effective cases of the Brauer-Siegel theorem*, Invent. Math., 23 (1974), pp. 135–152.
- [22] J. THORNER AND A. ZAMAN, *A Chebotarev variant of the Brun-Titchmarsh theorem and bounds for the Lang-Trotter conjectures*, 2016. Preprint. <http://arxiv.org/abs/1606.09238>.
- [23] M. WIDMER, *Counting primitive points of bounded height*, Trans. Amer. Math. Soc., 362 (2010), pp. 4793–4829.

K. DEBAENE, GEORG-AUGUST-UNIVERSITÄT GÖTTINGEN, BUNSENSTRASSE 3-5, 37073 GÖTTINGEN, GERMANY

*E-mail address*: [kdebaen@mathematik.uni-goettingen.de](mailto:kdebaen@mathematik.uni-goettingen.de)